REMARKS

In response to the Office Action mailed March 9, 2007, Applicants respectfully request reconsideration. Claims 1-43 were previously pending in this application. Claims 20-24 and 34-43 have been canceled without prejudice or disclaimer because they relate to a non-elected invention. Claims 25-33 have been amended. New claims 44-51 have been added. As a result, claims 1-19 and 25-51 are pending for examination with claims 1, 10, 20, 25 and 47 being independent claims. No new matter has been added.

Applicants respectfully request reconsideration.

Restriction

Applicants affirm the election of claims 1-19 and 25-33 in Group I. Having made this election, Applicants expressly reserve the right to file one or more divisional applications on the subject matter of the non-elected claims.

Rejections under 35 U.S.C. §101

Claim 25-33 are rejected under 35 U.S.C. §101. The claims have been amended to remove the Examiner's basis for the rejection and the rejection should be withdrawn.

Rejections Under 35 U.S.C. §103

Claims 1-19 and 25-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Abe et al., U.S. Publication No. 2005/0123138 (Abe) in view of Diffie et al., U.S. Patent No. 5,371,794 (Diffie). Applicants respectfully disagree.

As an aid to the Examiner, the Applicants provide a summary of the specification of the present application and of the Abe and Diffie references. This summary is not intended as a substitute for the Examiner reading the application and the references in their entireties. Also, the summary is not intended to characterize the claims or terms used in the claims, which are discussed individually below.

Briefly, as illustrated by FIG. 8, the present application describes a process by which hosts exchange messages using any of a number of modulation schemes. The modulation schemes are illustrated in FIG. 8 by $M_{1,}$ M_2... M_n. As illustrated in Table 1, the modulation schemes may encode different numbers of bits per symbol. Accordingly, because the messages exchanged use different modulation schemes, different number of bits may be communicated in each message.

In the example of FIG. 8, the first message communicates a set of bits B_0. In subsequent messages, sets of bits B_1, B_2... B_n are communicated. In this way, once the messages are communicated both of the hosts have access to sets of bits B_0, B_1... B_n. These sets of bits are used to construct on each host a key, identified as K_1 in FIG. 8. Once the hosts have exchanged enough bits so that each can construct a key, the hosts may thereafter communicate securely using that key.

For effective communication, the host that receives a message decodes the message using the same modulation scheme that was used by the host to send the message. An unauthorized listener to this exchange of messages does not know the modulation scheme used in each message and therefore cannot readily determine the bits forming the key that are communicated in each message. Though the modulation schemes may be changed randomly from message-to-message to make it more difficult for an unauthorized listener to guess the bits communicated in each message, each host knows which modulation scheme to use for each message it receives and can readily determine the bits that are used to form the key. Each host knows the modulation schemes of each message because each time a host communicates a set of bits, it also instructs the other host on which modulation scheme to use in a subsequent message.

For example, as illustrated in FIG. 8, when host A transmits a set of bits B_0, it also transmits an indication that modulation scheme M_1 should be used for a subsequent message. Accordingly, when host B sends a set of bits B_1, it encodes those bits using modulation scheme M_1. Along with the communication of bits B_1, host B sends to host A, including an indication that modulation scheme M_2 should be used for a subsequent communication. The process may continue in this fashion iteratively until a sufficient number of bits is communicated between host A and host B.

Though both the Abe and Diffie references deals generally with configuring wireless hosts with security encryption information, neither reference describes generating a cryptographic key in this fashion. For example, FIG. 1 of Abe shows a system with an encryption key generation section 151. However, rather than obtaining a key through a series of messages as described above, the encryption key generation section receives information from propagation estimating section 103. As described at ¶94, propagation estimating section 103 detects characteristics of a received signal, such as reception time, propagation time, frequency state, polarization state, reception power, multipath state, phase state or propagation distortion. As described at ¶120, such information defining a propagation state is used as an encryption key. Thus, the reference does not describe the iterative exchange of messages containing data used to generate an encryption key, transmitted using different modulation schemes, that is described in the present application.

The Examiner asserts that ¶¶109-111 and 152-154 describe receiving a second modulation scheme. However, ¶¶109-111 describe transmitting a reference signal. As understood, for the system of Abe to operate, each device estimates propagation characteristics of signals by receiving a reference signal sent by the other device. The passages cited by the Examiner describe transmission of such a reference signal.

Of course, Abe contains other differences from the system and method of the present application. The Examiner acknowledges that Abe does not describe that one modulation scheme is used to communicate an indication of another modulation scheme. Rather, the Examiner asserts that Diffie teaches this feature.

Diffie also described wirelessly establishing encryption information. However, that reference describes an alternative approach for exchanging keys wirelessly. As reflected in the Abstract and other portions of Diffie, Diffie's method involves exchanging and validating certificates, which allows two devices to reliably use public key encryption. By encrypting random numbers and other information, the process of Diffie results in both devices having access to a session key.

The Examiner asserts that Diffie at col. 8, lines 43 to col. 9, line 7 describes using different modulation schemes. However, the cited passage describes a portion of a process using private and session keys to encrypt or decrypt various messages. It does not describe different modulation schemes or using one modulation scheme to communicate an indication of a second modulation scheme.

As a result of these and other differences between the present application and the references, the references do not teach or suggest every limitation of any of the claims. For example, claim 1 recites "transmitting via the initial modulation scheme first data to be used in generating the cryptographic key and an indication of a second modulation scheme." Neither Abe's approach of using propagation state to generate a key nor Diffie's approach of using certificates in combination with public/private keys to communicate a session key meets this limitation of the claim. Accordingly, the claim is not anticipated nor obvious in light of the references.

Likewise, the references, whether alone or in combination, do not teach or suggest all limitations of independent claim 10. Claim 10 recites: "transmitting data between the first host and the second host using varying modulation schemes for each transmission; and generating the cryptographic key from the data."

As regards to independent claim 25, neither Abe nor Diffie, whether alone or in combination, teaches or suggests "transmitting via the initial modulation scheme first data to be used in generating a cryptographic key and an indication of a second modulation scheme."

As regards to newly added claim 47, Abe and Diffie, neither Abe nor Diffie, whether alone or in combination, teaches or suggests the iterative approach recited in the claim. Claim 47 expressly recites, for each of a plurality of iterations, "communicating a message between the first host and the second host using a modulation scheme, the message communicating a set of bits and a subsequent modulation scheme."

Each of the other claims remaining in the application depends directly or indirectly from one of these independent claims. Accordingly, the dependent claims distinguish over the references for at least the same reasons as the independent claims. The dependent claims also recite limitations that further distinguish the references.

For example, claim 2 depends from claim 1 and recites, in addition to the first and second modulation schemes, a third and fourth modulation scheme used to communicate data used in generating a cryptographic key. Because neither reference describes an iterative process of exchanging messages using different modulation schemes, neither describes four different modulation schemes.

As another example, claim 4 depends from claim 1 and further recites, determining the size of the cryptographic key and "selecting a final modulation scheme for a final data exchange" based on the size of the cryptographic key. No comparable function exists in either reference.

Other claims recite more specifically aspects of the modulation scheme. For example, claims 8 and 9 recite that selecting an initial modulation scheme includes "selecting an initial constellation" or "selecting an initial bit assignment for a constellation," respectively.

As yet another example, claim 44 depends from claim 1 and recites "***randomly*** selecting the second modulation scheme." No corresponding function occurs in either reference.

Thus, the dependent claims recite limitations providing further reasons why the rejection should be withdrawn.

As an additional reason why the references do not create a *prima facie* case of obviousness, there is no teaching, suggestion or other reason to combine elements from Abe and Diffie as the Examiner has done. As described above, Abe teaches a method of using estimations of propagation state to exchange encryption keys between two devices. Diffie describes an alternative approach for exchanging cryptographic keys between devices. The references teach alternative approaches to solving the same problem. If one of skill in the art were to consider the references in their entireties, one of skill in the art would select either approach of Abe or the approach of Diffie, but not pick and choose elements of both. Accordingly, there is no reason to incorporate elements of Diffie into the system of Abe as done by the Examiner in formulating the rejection.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: June 11, 2007

Respectfully submitted,

By: ____________________
Edmund J. Walsh
Registration No. 32,950
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000